



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : G07F 7/10, H04L 9/08	A1	(11) Numéro de publication internationale: WO 98/40853
		(43) Date de publication internationale: 17 septembre 1998 (17.09.98)

(21) Numéro de la demande internationale: PCT/FR98/00503

(22) Date de dépôt international: 12 mars 1998 (12.03.98)

(30) Données relatives à la priorité:
97/02973 13 mars 1997 (13.03.97) FR(71) Déposant (pour tous les Etats désignés sauf US): BULL CP8
[FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430
Louveciennes (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (US seulement): HAZARD, Michel
[FR/FR]; 27, rue des Harias, F-78124 Mareil sur Mauldre
(FR).(74) Mandataire: CORLU, Bernard; Bull S.A., PC59C18, 68, route
de Versailles, F-78434 Louveciennes Cedex (FR).(81) Etats désignés: AU, BR, CA, CN, JP, KR, NO, SG, US, brevet
européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE).

Publiée

Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des
revendications, sera republiée si de telles modifications sont
requises.

(54) Title: METHOD FOR STORING AND OPERATING SENSITIVE INFORMATION IN A SECURITY MODULE, AND ASSOCIATED SECURITY MODULE

(54) Titre: PROCÉDE DE STOCKAGE ET D'EXPLOITATION D'UNE INFORMATION SENSIBLE DANS UN MODULE DE SECURITE, ET MODULE DE SECURITE ASSOCIE

1	2	3	4	5	6
Référence des informations sensibles	Numéro de la clé associée	Indice actuel de la clé	version stockée de l'information sensible	Nouvel indice de la clé	nouvelle version stockée de l'information sensible
IS1	N1	a1+1	IS1(act+1)		
IS2	N1	a1+1	IS1(act+1)		
.
.
.
IS(j-1)	Nj	aj+1	IS(j-1)(act+1)	aj+2	IS(j-1)(act+2)
ISj	Nj	aj+1	ISj(act+1)	aj+2	ISj(act+2)
.
.
.
ISm	Nn	an+1	ISm(act+1)		

- 1...SENSITIVE INFORMATION REFERENCE
2...ASSOCIATED KEY NUMBER
3...PRESENT KEY INDEX
4...STORED VERSION OF SENSITIVE INFORMATION
5...NEW KEY INDEX
6...NEW STORED VERSION OF SENSITIVE INFORMATION

(57) Abstract

The invention concerns a method for storing and operating sensitive information in a security module, and a security module arranged for implementing this method, aimed at protecting this sensitive information against fraudulent use. The method is characterised in that it consists in storing the sensitive information IS_j in encrypted form IS_j using a temporary protection encryption key CPI, whose content varies in time. The sensitive information IS_j is decrypted before it is used in a given process, by means of a temporary protection decryption key CPid. Before the contents of the encryption and decryption keys is changed, the sensitive information IS_j is decrypted with the current decryption key, then it is reencrypted with the new encryption key to obtain a new encrypted form, different from the previous one.

(57) Abrégé

L'invention est relative à un procédé de stockage et d'exploitation d'une information sensible dans un module de sécurité, et à un module de sécurité agencé pour mettre en oeuvre ce procédé, visant à protéger cette information sensible vis-à-vis d'une utilisation frauduleuse. Selon ce procédé, on stocke l'information sensible ISj sous une forme chiffrée ISj au moyen d'une clé de protection temporaire de chiffrement CPI, dont le contenu varie dans le temps. On déchiffre l'information sensible ISj avant son utilisation dans un traitement donné, au moyen d'une clé de protection temporaire de déchiffrement CPid. Avant de faire varier le contenu des clés de chiffrement et déchiffrement, on déchiffre l'information sensible ISj avec la clé de déchiffrement actuelle, puis on la rechiffre avec la nouvelle clé de chiffrement pour obtenir une nouvelle forme chiffrée, différente de la précédente.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

Procédé de stockage et d'exploitation d'une information sensible dans un module de sécurité, et module de sécurité associé

L'invention concerne un procédé de stockage et d'exploitation d'une
5 information sensible dans un module de sécurité, ainsi que le module de sécurité associé.

Le terme « information sensible » désigne en premier lieu toute information dont la connaissance a des répercussions significatives sur la sécurité des opérations mises en oeuvre dans le module de sécurité, comme par exemple :

- 10 - des clés cryptographiques utilisées en association avec des algorithmes dans des opérations de chiffrement ou déchiffrement d'un message, d'authentification d'une donnée ou d'une personne, ou de signature d'un message ;
- des codes d'authentification présentés par un usager auprès d'un terminal coopérant avec le module de sécurité (par exemple le "P.I.N", dérivé de l'anglais
15 "Personal Identification Number") ;

Par extension, le terme "information sensible" désigne aussi toute information jugée confidentielle par celui qui la détient, comme par exemple un numéro de compte bancaire, un message, ou même l'ensemble d'un document.

Le terme "module de sécurité" doit être pris, soit dans son sens classique
20 dans lequel il désigne un dispositif ayant vocation, dans un réseau de communication ou d'information, à être détenu par un organisme supervisant le réseau et à stocker de façon protégée des paramètres secrets et fondamentaux du réseau tels que des clés cryptographiques, soit comme désignant plus simplement un dispositif attribué à divers usagers du réseau et permettant à chacun d'eux
25 d'avoir accès à celui-ci, ce dernier dispositif étant lui aussi susceptible de détenir des paramètres secrets. Le module de sécurité pourra prendre la forme d'un objet portatif du type carte à puce, tel qu'une carte bancaire.

L'invention part de la constatation que, à l'aide de moyens en matériel accessibles à tous, un fraudeur peut observer la consommation de courant du
30 module de sécurité lors de l'exécution d'un programme ou d'instructions définies par une logique micro-câblée dans le module de sécurité, surtout quand ce dernier est de technologie CMOS. Il est notamment possible d'identifier des portions particulières du programme qui assurent la lecture d'informations en mémoire EEPROM, en particulier les informations sensibles définies ci-dessus.

L'invention vise donc à renforcer la sécurité des modules de sécurité, au sens précisé ci-dessus, en assurant la protection des informations sensibles, notamment lors de leur transfert entre une mémoire EEPROM et une mémoire RAM où l'inverse, en les chiffrant au moyen d'une clé de protection temporaire dont le contenu varie à une certaine fréquence, notamment une fréquence qui est fonction du degré de confidentialité de l'information sensible.

Elle concerne à cet effet un procédé de stockage d'une information sensible IS_j dans un module de sécurité comprenant des moyens de traitement de l'information et des moyens de mémorisation de l'information, caractérisé en ce qu'il comprend les étapes consistant à :

-faire chiffrer l'information sensible IS_j par le module de sécurité au moyen d'une clé de protection temporaire de chiffrement CP_i dans une version actuelle CP_{i(ai+1)} fournie par le module de sécurité et d'un algorithme de chiffrement stocké, avec un algorithme de déchiffrement associé, dans lesdits moyens de mémorisation ;

-faire stocker par le module de sécurité, dans une mémoire non volatile de celui-ci, l'information sensible sous forme chiffrée \overline{IS}_j _(ai+1) associée à des données d'identification définissant une clé de protection temporaire de déchiffrement CP_{id} dans une version actuelle CP_{id(ai+1)} associée à ladite version actuelle CP_{i(ai+1)} de la clé de protection temporaire de chiffrement CP_i, lesdites données d'identification comprenant une identité de clé CP_{id} et un indice de mise à jour (ai+1) qui définit ladite version actuelle CP_{id(ai+1)} de la clé de déchiffrement parmi plusieurs versions ; et

-dans le cas où la clé de protection temporaire de déchiffrement CP_{id} dans sa version actuelle CP_{id(ai+1)} n'est pas déjà stockée dans ladite mémoire non volatile, faire stocker cette version par le module de sécurité.

L'invention concerne aussi un procédé d'exploitation d'une information sensible IS_j dans un module de sécurité comprenant des moyens de traitement de l'information et des moyens de mémorisation de l'information, cette information sensible IS_j étant sous une forme chiffrée par le module de sécurité au moyen d'une clé de protection temporaire de chiffrement CP_i dans une version actuelle CP_{i(ai+1)} fournie par le module de sécurité et d'un algorithme de chiffrement stocké, avec un algorithme de déchiffrement associé, dans lesdits moyens de

mémorisation, l'information sensible sous forme chiffrée $\overline{ISj}_{(ai+1)}$ étant stockée dans une mémoire non volatile du module de sécurité en association avec des données d'identification définissant une clé de protection temporaire de déchiffrement CPid dans une version actuelle $CPid_{(ai+1)}$ associée à ladite version actuelle $CPI_{(ai+1)}$ de la

5 clé de protection temporaire de chiffrement CPI, lesdites données d'identification comprenant une identité de clé CPid et un indice de mise à jour (ai+1) qui définit ladite version actuelle $CPid_{(ai+1)}$ de la clé de déchiffrement parmi plusieurs versions, caractérisé en ce qu'il comprend les étapes consistant à :

-faire sélectionner par le module de sécurité, à chaque demande d'utilisation

10 de l'information sensible ISj émanant de l'intérieur ou de l'extérieur de celui-ci, ladite version actuelle $CPid_{(ai+1)}$ de la clé de protection temporaire de déchiffrement CPid associée à cette information sensible, au moyen desdites données d'identification ;

-faire déchiffrer par le module de sécurité l'information sensible chiffrée

15 $\overline{ISj}_{(ai+1)}$, au moyen de la version actuelle $CPid_{(ai+1)}$ de la clé de protection temporaire de déchiffrement CPid et de l'algorithme de déchiffrement, et stocker provisoirement l'information sensible ISj sous une forme déchiffrée ainsi obtenue de telle façon qu'elle disparaisse du module de sécurité après une utilisation de cette information sensible ; et

20 -faire utiliser par le module de sécurité l'information sensible ISj sous sa forme déchiffrée.

L'invention concerne enfin un module de sécurité agencé pour mettre en oeuvre les procédés ci-dessus.

D'autres détails et avantages de la présente invention apparaîtront au cours

25 de la description suivante d'un mode d'exécution préféré mais non limitatif, en regard des dessins annexés sur lesquels :

La figure 1 est le schéma d'un module de sécurité auquel est destinée l'invention, coopérant avec un dispositif de traitement de l'information ;

La figure 2 est un tableau présentant un jeu de clés de protection

30 temporaires et différents attributs de celles-ci ;

La figure 3 est un tableau présentant un ensemble d'informations sensibles et les clés de protection temporaires qui leur sont attribuées respectivement ;

La figure 4 est un organigramme d'une procédure de chiffrement initial d'une quelconque information sensible ISj ;

La figure 5 est un organigramme d'une procédure de déchiffrement de l'information sensible $\overline{IS_j}$, en vue de son utilisation dans un traitement ;

La figure 6 est un organigramme d'une procédure de rafraîchissement périodique d'une quelconque clé de protection temporaire CPi ;

5 Les figures 7 et 8 représentent des tableaux correspondant respectivement à ceux des figures 2 et 3, mais comportant des clés de protection temporaires ou des informations sensibles rafraîchies ; et

La figure 9 est un organigramme d'une procédure de rafraîchissement périodique d'une quelconque information sensible.

10

Le dispositif de traitement de l'information 1 représenté sur la figure 1 comprend de façon connue en soi un microprocesseur 2 auquel sont reliés une mémoire ROM 3, et une mémoire RAM 4, des moyens 5 pour coopérer, avec ou sans contact physique, avec un module de sécurité 8, et une interface de transmission 7 permettant au dispositif de traitement de l'information de
15 communiquer avec un autre dispositif semblable, soit directement, soit au travers d'un réseau de communication.

Le dispositif 1 peut en outre être équipé de moyens de stockage tels que des disquettes ou disques amovibles ou non, de moyens de saisie (tels qu'un
20 clavier et/ou un dispositif de pointage du type souris) et de moyens d'affichage, ces différents moyens n'étant pas représentés sur la figure 1.

Le dispositif de traitement de l'information peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services,
25 cet appareil étant installé à demeure ou portable. Il peut notamment s'agir aussi d'un appareil de télécommunications.

Par ailleurs, le module de sécurité 8 inclut des moyens de traitement de l'information 9, une mémoire non volatile 10, une mémoire volatile de travail RAM 14, et des moyens 13 pour coopérer avec le dispositif de traitement de
30 l'information. Ce module est agencé pour définir, dans la mémoire 10, une zone secrète 11 dans laquelle des informations une fois enregistrées, sont inaccessibles depuis l'extérieur du module mais seulement accessibles aux moyens de traitement 9, et une zone libre 12 qui est accessible depuis l'extérieur du module pour une lecture et/ou une écriture d'informations. Chaque zone de la mémoire non

volatile 10 peut comprendre une partie non modifiable ROM et une partie modifiable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash", c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM classique.

5 En tant que module de sécurité 8, on pourra notamment utiliser un microprocesseur à mémoire non volatile autoprogrammable, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Comme indiqué en colonne 1, lignes 13-25 de ce brevet, le caractère autoprogrammable de la mémoire correspond à la possibilité pour un programme fi situé dans cette
10 mémoire, de modifier un autre programme fj situé également dans cette mémoire en un programme gj. Bien que les moyens à mettre en oeuvre pour réaliser cette autoprogrammation puissent varier selon la technique utilisée pour concevoir les moyens de traitement de l'information 9, on rappelle que, dans le cas où ces moyens de traitement sont constitués par un microprocesseur associé à une
15 mémoire non volatile et selon le brevet précité, ces moyens peuvent inclure :

- des mémoires tampon de données et d'adresses, associées à la mémoire ;
- un programme d'écriture dans la mémoire, chargé dans celle-ci et contenant notamment les instructions permettant le maintien d'une part de la tension de programmation de la mémoire, et d'autre part des données à écrire et
20 de leurs adresses, pendant un temps suffisant, ce programme d'écriture pouvant toutefois être remplacé par un automate d'écriture à circuits logiques.

Dans une variante, le microprocesseur du module de sécurité 8 est remplacé -ou tout du moins complété- par des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des
25 calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »). A titre d'exemple, on peut citer le composant de la société SIEMENS commercialisé sous la référence SLE 4436 et celui de la société SGS-THOMSON commercialisé sous la référence ST 1335.

30 Avantageusement, le module de sécurité 8 sera conçu sous forme monolithique sur une seule puce.

En variante au microprocesseur à mémoire non volatile autoprogrammable décrit ci-dessus, le caractère sécuritaire du module de sécurité pourra résulter de sa localisation dans une enceinte inviolable.

L'invention met en oeuvre plusieurs clés de protection temporaires de chiffrement $CP_1, \dots, CP_i, \dots, CP_n$ et plusieurs clés de protection temporaires de déchiffrement associées $CPd_1, \dots, CPd_i, \dots, CPd_n$. Selon le type d' algorithme de

5 chiffrement utilisé, les clés de protection temporaires de déchiffrement sont identiques aux clés de protection temporaires de chiffrement ou bien différentes de celles-ci. Ainsi, en tant qu'algorithme de chiffrement , on utilisera typiquement un algorithme symétrique à clé secrète, tel que l'algorithme DES (de l'anglais Data Encryption Standard), la clé secrète correspondant à l'une des clés de protection

10 temporaires de chiffrement $CP_1, \dots, CP_i, \dots, CP_n$. Pour ce type d'algorithmes, on utilise un algorithme de déchiffrement qui est égal à l'inverse de l'algorithme de chiffrement, et la clé secrète est utilisée indifféremment pour le chiffrement et le déchiffrement. En d'autres termes, l'opération de déchiffrement utilise une clé de déchiffrement qui est identique à la clé de chiffrement.

15 Dans une variante moins avantageuse, on utilise un algorithme asymétrique à clé publique, tel que l'algorithme RSA (des inventeurs Rivest, Shamir, et Adleman) qui met en oeuvre une clé de chiffrement publique et une autre clé de déchiffrement secrète, différente de la clé de chiffrement. Dans ce cas, le module de sécurité stocke ces deux clés, ou des paramètres permettant de les

20 reconstituer, selon deux versions successives.

Dans la description des figures qui va suivre, on utilise un algorithme symétrique à clé secrète, de sorte que les clés de protection temporaires de déchiffrement $CPd_1, \dots, CPd_i, \dots, CPd_n$ se confondent avec les clés de protection temporaires de chiffrement $CP_1, \dots, CP_i, \dots, CP_n$; pour cette raison, les notations

25 $CPd_1, \dots, CPd_i, \dots, CPd_n$ ne sont pas utilisées et sont remplacées par $CP_1, \dots, CP_i, \dots, CP_n$ appelées alors simplement « clés de protection temporaires » sans préciser leur rôle de chiffrement ou déchiffrement.

L'algorithme de chiffrement pourra être identique à un algorithme utilisé pour différentes fonctions relatives aux applications auxquelles est destiné le

30 module de sécurité , ou bien être spécifique et dédié à la tâche de chiffrement des clés de protection temporaires.

Le tableau de la figure 2 comprend une première colonne définissant un nombre n de clés de protection temporaires $CP_1, \dots, CP_i, \dots, CP_n$ portant respectivement un numéro de clé $N_1, \dots, N_i, \dots, N_n$ servant à les désigner. En vue

de parer à toute interruption de traitement intempestive du module de sécurité, et comme précisé par la suite, on stocke, pour chaque clé de protection temporaire, deux valeurs successives de la clé repérées chacune par un indice de mise à jour relatif à cette clé et repéré par $a_1, \dots, a_i, \dots, a_n$. Cet indice de mise à jour a pour

5 valeur un rang de mise à jour. Ainsi, la clé CP_i a une valeur actuelle $CP_{i(a_i+1)}$ définie par un indice de mise à jour (a_i+1) , et une valeur $CP_{i a_i}$ immédiatement antérieure dans le temps et définie par un indice de mise à jour (a_i) . Les différents indices de mise à jour évoluent indépendamment les uns des autres.

Le tableau de la figure 3 comprend, dans une première colonne, des

10 références d'un nombre m d'informations sensibles $IS_1, IS_2, \dots, IS_{(j-1)}, IS_j, \dots, IS_m$, chacune étant stockée dans le module de sécurité sous forme chiffrée au moyen d'un algorithme de chiffrement et d'une clé de protection temporaire choisie parmi celles du tableau de la figure 2. Une deuxième colonne du tableau définit le

15 numéro de la clé de protection temporaire utilisée pour chaque information sensible. Ainsi, la clé de protection temporaire CP_1 (dont le numéro est N_1) est utilisée pour protéger les informations sensibles IS_1, IS_2 , la clé de protection temporaire CP_i pour les informations sensibles $IS_{(j-1)}, IS_j$, et la clé de protection temporaire CP_n pour la seule information sensible IS_m . Une troisième colonne du

20 tableau précise l'indice de mise à jour que la clé de protection temporaire avait lorsqu'elle a été utilisée pour chiffrer l'information sensible. Ainsi, les informations sensibles $IS_1, IS_2, \dots, IS_j, \dots, IS_m$ ont été chiffrées avec une clé portant le plus récent indice de mise à jour $(a_1+1), (a_i+1)$, ou (a_n+1) selon les cas, tandis que l'information sensible $IS_{(j-1)}$ a été chiffrée avec une clé portant un indice de mise à jour (a_i) précédant le plus récent indice de mise à jour (a_i+1) . Enfin, une quatrième

25 colonne du tableau indique la version stockée de l'information sensible. Ainsi, l'information sensible IS_j est stockée sous la forme chiffrée $\overline{IS_j}_{(a_i+1)}$ qui porte l'indice de mise à jour (a_i+1) relatif à la clé de protection temporaire associée.

Typiquement, les données contenues dans les tableaux des figures 2 et 3 sont stockées dans la mémoire non volatile 10 du module de sécurité, les valeurs

30 des clés de protection temporaires telles que $CP_{i a_i}$ étant stockées en zone secrète 11 tandis que les autres données peuvent être stockées, soit de préférence en zone secrète 11, soit en zone libre 12. En ce qui concerne la taille de ces données exprimée en bits, la taille des clés, qu'il s'agisse des clés de protection temporaires CP_i ou de clés constituant les informations sensibles IS_j , sera

typiquement de 64 bits, tandis que celle des numéros Ni et indices de mise à jour(ai) sera typiquement d'1 octet. On notera que la première colonne du tableau de la figure 2 peut ne pas être stockée dans le module de sécurité, mais son stockage peut néanmoins être utile pour définir le type d'information dont il s'agit, si on souhaite stocker les clés de protection temporaires dans une zone contenant des informations d'un autre type.

Chaque clé de protection temporaire telle que CPi possède une valeur qui évolue dans le temps et est générée en interne par le module de sécurité. Selon une forme préférée de réalisation, chaque clé CPi est un aléa ou une fonction d'un aléa produit par le module de sécurité, de sorte que son évolution dans le temps est imprévisible. Cet aléa pourra être généré de façon logicielle, par exemple selon l'un des procédés décrits dans les brevets américains N°5.177.790 ou 5.365.466, ou au moyen d'un circuit produisant une grandeur physique aléatoire. Selon une forme moins préférée de réalisation, chaque clé CPi est une donnée qui évolue dans le temps selon une règle prédéterminée. Par exemple, cette donnée est égale au contenu d'un compteur qui est régulièrement incrémenté d'une unité. Selon les situations, chaque clé de protection temporaire CPi sera générée soit à l'avance, soit au moment de son utilisation pour chiffrer une information sensible ISj. Dans tous les cas, la création des clés de protection temporaires CPi ainsi que le chiffrement ou déchiffrement des informations sensibles ISj sont sous le seul contrôle du module de sécurité ou parfois d'une autorité spécialement habilitée, coopérant avec le module de sécurité, en ce sens que seuls le module de sécurité ou cette autorité prennent la décision d'effectuer ces opérations qui sont transparentes pour le monde extérieur non habilité (c'est-à-dire tout terminal et usager ordinaires coopérant avec le module de sécurité), même si ces opérations peuvent être déclenchées indirectement par une demande de ce monde extérieur non habilité visant par exemple à faire intervenir une information sensible ISj dans un calcul cryptographique tel que le chiffrement ou la signature d'un message, ou l'authentification d'un message ou d'une personne.

Le cas le plus fréquent est celui où le module de sécurité coopère avec un terminal non habilité et contrôle lui-même la création des clés de protection temporaires CPi ainsi que le chiffrement ou déchiffrement des informations sensibles ISj. Un cas moins fréquent est celui où le module de sécurité coopère avec un terminal de l'autorité habilitée, soit avant une première utilisation du

module de sécurité pour initialiser celui-ci, soit au cours de sa durée de vie pour permettre à l'autorité habilitée de contrôler le module de sécurité ou de modifier des fonctions ou données qu'il contient ; dans ce dernier cas, la création des clés de protection temporaires CPI ainsi que le chiffrement ou déchiffrement des informations sensibles IS_j peuvent éventuellement être sous le contrôle de cette autorité, et non plus du module de sécurité.

La figure 4 est un organigramme d'une procédure de chiffrement initial d'une quelconque information sensible IS_j , avant son stockage en mémoire non volatile du module de sécurité. Un exemple typique est le cas où cette procédure est déclenchée depuis l'extérieur du module de sécurité, par une autorité désirant stocker dans celui-ci l'information sensible IS_j . Dans une première étape 41, le module de sécurité stocke en mémoire de travail 14 la nouvelle information sensible IS_j reçue de l'extérieur, tandis que dans une deuxième étape 42, le module de sécurité -ou éventuellement l'autorité habilitée -décide si une nouvelle clé de protection temporaire CPI ou une clé existante sera utilisée pour chiffrer l'information sensible IS_j . Dans la négative, les moyens de traitement 9 du module de sécurité sélectionnent (étape 43) une clé de protection temporaire existant en mémoire non volatile 10 et la transfèrent (étape 44) en mémoire de travail volatile 14. Selon l'exemple de la figure 3, il s'agit de la clé CPI , portant le numéro N_i . Le module de sécurité choisit, en tant que valeur de clé, celle qui est à l'indice de mise à jour le plus élevé : en l'espèce, il s'agit de l'indice $(ai+1)$, mais si cette clé n'avait jamais été mise à jour, il s'agirait de l'indice 1. Si, au contraire, il est décidé à l'étape 42 qu'une nouvelle clé de protection temporaire doit être créée, cette création par le module de sécurité s'effectue à l'étape 45 en mémoire de travail 14 et la clé est sauvegardée (étape 46) en mémoire non volatile pour un usage ultérieur.

A l'étape 47, le module de sécurité chiffre l'information IS_j avec la clé CPI pour obtenir un résultat $\overline{IS_j}_{(ai+1)}$. A l'étape 48, le module de sécurité stocke ce résultat dans une zone de la mémoire non volatile dédiée à cette information sensible. Naturellement, le module de sécurité stocke, en association avec l'information sensible $\overline{IS_j}_{(ai+1)}$ et comme illustré sur la figure 3, le numéro N_i et l'indice de mise à jour $(ai+1)$ de la clé utilisée.

La figure 5 est un organigramme d'une procédure de déchiffrement de l'information sensible $\overline{IS_j}$, en vue de son utilisation dans un traitement, typiquement un traitement interne au module de sécurité. A l'étape 51, une demande d'utilisation d'une information sensible IS_j est formulée, par exemple à l'initiative du dispositif de traitement de l'information 1, de sorte qu'à l'étape 52, le module de sécurité transfère l'information sensible sous sa forme chiffrée $\overline{IS_j}_{(ai+1)}$ et la clé de protection temporaire correspondante CPI (dans la version applicable $ai+1$) depuis sa mémoire non volatile 10 dans sa mémoire de travail 14. Il y déchiffre alors (étape 53) l'information sensible avec la clé pour obtenir l'information sensible déchiffrée IS_j . A l'étape 54, le module de sécurité utilise l'information sensible déchiffrée IS_j dans le traitement à effectuer. On notera qu'après utilisation dans le traitement à effectuer, l'information sensible déchiffrée IS_j disparaîtra de façon qu'elle ne réside pas durablement dans le module de sécurité. Ceci est obtenu, dans cet exemple, grâce à une propriété d'une mémoire volatile selon laquelle les informations qu'elle contient disparaissent lors de sa mise hors tension intervenant à la fin de la communication avec le dispositif de traitement de l'information 1.

La figure 6 est un organigramme d'une procédure de rafraîchissement (c'est-à-dire de renouvellement) périodique d'une quelconque clé de protection temporaire CPI . Son intérêt réside notamment en ce qu'une variation du contenu de cette clé est ainsi produite, rendant très difficile toute tentative frauduleuse pour deviner cette clé ; de plus, cette clé rafraîchie permettra, par un nouveau chiffrement des informations sensibles associées, de rafraîchir la forme chiffrée de celles-ci, rendant d'autant plus difficile toute tentative frauduleuse pour deviner le contenu des informations sensibles à partir de leur forme chiffrée. En effet, on sait qu'un fraudeur peut éventuellement tirer parti de l'observation des signaux électriques présents aux bornes du module de sécurité, notamment durant les transferts de données entre la mémoire non volatile et la mémoire de travail 14, signaux qui sont en pratique toujours influencés par la nature des traitements effectués par le module de sécurité. Moyennant le stockage par le fraudeur d'un nombre important de telles observations et une analyse statistique, celui-ci peut éventuellement parvenir à reconstituer les informations sensibles concernées.

La procédure de la figure 6 est déclenchée, soit à l'initiative du module de sécurité qui est agencé pour rafraîchir ses clés de protection temporaires à un

rythme prédéterminé voire aléatoire, soit à l'initiative du dispositif de traitement de l'information 1 qui envoie à cet effet au module de sécurité un message ou une commande appropriée, bien que dans ce dernier cas, l'exécution proprement dite de la procédure demeure sous le seul contrôle du module de sécurité, sauf

5 éventuellement dans le cas particulier où le dispositif de traitement de l'information 1 est celui de l'autorité habilitée. Le rafraîchissement est effectué à un rythme qui est de préférence fonction du type d'information sensible considéré : ainsi, ce rythme sera élevé pour une information sensible telle qu'un code confidentiel d'utilisateur ou « PIN » (de l'anglais Personal Identification Number) qui, compte tenu

10 du faible nombre de chiffres qu'il comporte habituellement et de son utilisation fréquente, est davantage sujet à la fraude qu'une clé cryptographique de chiffrement ou de signature. Le module de sécurité stockera avantageusement, dans sa mémoire non volatile 10, des indications sur le rythme de rafraîchissement à appliquer à chaque information sensible. Par exemple, le rafraîchissement

15 pourra être prévu à chaque fois que l'information sensible considérée aura été utilisée un nombre prédéterminé de fois.

Dans une première étape 61, le module de sécurité consulte son tableau de la figure 2 pour déterminer si la clé de protection temporaire CPI qu'il doit rafraîchir est à l'indice de mise à jour le plus élevé pour toutes les informations sensibles

20 qu'elle protège. En effet, sachant qu'on souhaite ne conserver de préférence, pour chaque clé, que deux versions successives, le rafraîchissement d'une clé suppose l'effacement de la version la plus ancienne pour écrire à la place la version la plus récente ; or, cet effacement ne peut se faire que si aucune information sensible stockée actuellement n'aura besoin d'être déchiffrée au moyen de la version la

25 plus ancienne, faute de quoi ce déchiffrement ne sera pas possible.

Si la condition posée à l'étape 61 n'est pas remplie, le module de sécurité va procéder à une mise à jour de la forme chiffrée des informations sensibles concernées. Tout d'abord, à l'étape 62, il transfère en mémoire de travail 14 ces informations sensibles (dans cet exemple, la seule information sensible $\overline{IS(j-1)}_{ai}$),

30 la valeur correspondante CPI_{ai} de la clé de protection temporaire CPI , et la valeur la plus récente $CPI_{(ai+1)}$ de cette même clé. A l'étape 63, il déchiffre l'information sensible $\overline{IS(j-1)}_{ai}$ avec la clé CPI_{ai} puis, à l'étape 64, il sauvegarde l'information sensible $\overline{IS(j-1)}_{ai}$ (c'est-à-dire sous sa forme chiffrée) dans une zone tampon de

la mémoire non volatile 10, pour éviter de la perdre au cas où le rechargement subséquent de $IS(j-1)$ serait interrompu. A l'étape 65, le module de sécurité recharge l'information sensible $IS(j-1)$ restituée avec la valeur la plus récente $CPI_{(ai+1)}$ de la clé de protection temporaire CPI pour obtenir une version la plus récente $\overline{IS(j-1)}_{(ai+1)}$ de la forme chiffrée de l'information sensible $IS(j-1)$. Enfin, à l'étape 66, le module de sécurité remplace, en mémoire non volatile 10, la valeur la plus ancienne $\overline{IS(j-1)}_{ai}$ par la valeur la plus récente $\overline{IS(j-1)}_{(ai+1)}$ et il met à jour l'indice de mise à jour (ai) en l'incrémentant d'une unité pour obtenir ($ai+1$) : cette situation est illustrée en caractères gras sur la figure 8, troisième et quatrième colonnes du tableau.

Après cette étape, ou si la condition de l'étape 61 était déjà satisfaite, le module de sécurité génère, à l'étape 67, une nouvelle valeur $CPI_{(ai+2)}$ de la clé de protection temporaire CPI à un nouvel indice de mise à jour ($ai+2$) en mémoire de travail 14. Comme indiqué précédemment, selon un mode préféré de réalisation, cette nouvelle valeur est un aléa ou une fonction d'un aléa. Enfin, à l'étape 68, le module de sécurité remplace, dans son tableau de la figure 2 situé en mémoire non volatile 10, la plus ancienne valeur CPI_{ai} de la clé de protection temporaire CPI par la plus récente $CPI_{(ai+2)}$ et il met à jour l'indice de mise à jour (ai) en l'incrémentant de deux unités pour obtenir ($ai+2$) : cette situation est illustrée en caractères gras sur la figure 7, troisième et quatrième colonnes du tableau..

La figure 9 est un organigramme d'une procédure de rafraîchissement périodique d'une quelconque information sensible. Typiquement, cette procédure fera suite à la procédure de rafraîchissement de clés de la figure 6 et concernera précisément les informations sensibles associées aux clés ainsi rafraîchies ; toutefois, en variante, elle pourra être exécutée à tout moment ultérieur. Elle sera déclenchée, comme la procédure de la figure 6, soit à l'initiative du module de sécurité qui est agencé pour rafraîchir ses informations sensibles à un rythme prédéterminé voire aléatoire, soit à l'initiative du dispositif de traitement de l'information 1 qui envoie à cet effet au module de sécurité un message ou une commande appropriée, bien que dans ce dernier cas, l'exécution proprement dite de la procédure demeure sous le seul contrôle du module de sécurité, sauf éventuellement dans le cas particulier où le dispositif de traitement de l'information 1 est celui de l'autorité habilitée.

A l'étape 91, une demande de rafraîchissement d'informations sensibles est donc formulée. A l'étape 92, le module de sécurité transfère les informations sensibles considérées et leurs clés de protection temporaires associées en mémoire de travail 14 : dans cet exemple, il s'agit des informations sensibles

5 $\overline{IS(j-1)}_{(ai+1)}$ et $\overline{ISj}_{(ai+1)}$, et des clés $CPI_{(ai+1)}$ et $CPI_{(ai+2)}$. A l'étape 93, le module de sécurité déchiffre ces informations sensibles avec la clé $CPI_{(ai+1)}$, puis, à l'étape 94, il rechiffre les informations sensibles $IS(j-1)$ et ISj ainsi obtenues avec la clé $CPI_{(ai+2)}$. A l'étape 95, il stocke les informations sensibles rechiffrées $\overline{IS(j-1)}_{(ai+2)}$ et $\overline{ISj}_{(ai+2)}$ dans la zone tampon précitée de la mémoire non volatile. Enfin, à l'étape

10 96, il stocke ces données dans la zone dédiée de la mémoire non volatile, à la place des informations sensibles $\overline{IS(j-1)}_{(ai+1)}$ et $\overline{ISj}_{(ai+1)}$, et il met à jour l'indice de mise à jour ($ai+1$) en l'incrémentant d'une unité pour obtenir ($ai+2$) : cette situation est illustrée en caractères gras sur la figure 8, cinquième et sixième colonnes du tableau.

15 En ce qui concerne les différentes procédures décrites ci-dessus, l'enchaînement des étapes pourra être éventuellement provisoirement interrompu par les moyens de traitement de l'information 9 du module de sécurité pour exécuter d'autres tâches, indépendantes du procédé de l'invention mais jugées prioritaires à un moment donné. Dans ce cas, la procédure sera reprise dès la fin

20 d'exécution de ces tâches. Par ailleurs, l'ordre dans lequel le module de sécurité traitera les clés de protection temporaires et les informations sensibles pourra changer selon différentes variantes. Par exemple, la procédure de la figure 6 effectue un rafraîchissement complet de la clé CPI , indépendamment de celui des autres clés ; dans une variante, le module de sécurité effectue un rafraîchissement

25 simultané de plusieurs clés, les étapes de la figure 6 propres à chaque clé se trouvant alors juxtaposées ou imbriquées avec celles propres aux autres clés.

En ce qui concerne la façon de faire disparaître l'information sensible déchiffrée, après son utilisation dans un traitement donné, l'exemple ci-dessus a utilisé la propriété de perte des informations d'une mémoire volatile (ici, la mémoire

30 de travail 14) lors de sa mise hors tension, à la fin de la communication avec le dispositif de traitement de l'information 1. En variante, si la mémoire utilisée pour le stockage provisoire de l'information sensible n'était pas volatile, il y aurait lieu de déclencher un effacement de cette information en mémoire, au moyen d'un ordre

spécifique exécuté par le microprocesseur 9 du module de sécurité. L'expression « stocker provisoirement l'information sensible déchiffrée de telle façon qu'elle disparaisse du module de sécurité après utilisation », employée à certains endroits du présent texte, vise à couvrir notamment ces deux formes d'exécution.

5 Dans le cas de la variante de l'invention évoquée précédemment et utilisant un algorithme asymétrique à clé publique, un tel algorithme reçoit typiquement des données selon un format de 512 bits, c'est-à-dire sensiblement supérieur au format typique des informations sensibles (64 bits). Avantageusement, on procède alors à un regroupement ou concaténation de plusieurs informations sensibles pour
10 atteindre un format d'ensemble de 512 bits, avant leur chiffrement commun par ledit algorithme.

Dans l'exemple décrit ci-dessus, le module de sécurité 8 fonctionne typiquement dans un mode accouplé avec un dispositif de traitement de l'information 1. En variante, le module de sécurité possède des moyens d'auto-
15 alimentation en énergie électrique et met en oeuvre le procédé décrit ci-dessus de stockage ou d'exploitation d'une information sensible -ou au moins certaines étapes de celui-ci- dans un mode autonome, c'est-à-dire non accouplé avec un dispositif de traitement de l'information.

REVENDEICATIONS

1. Procédé de stockage d'une information sensible IS_j dans un module de sécurité (8) comprenant des moyens de traitement de l'information (9) et des moyens de mémorisation de l'information (10,14), caractérisé en ce qu'il comprend

5 les étapes consistant à :

-faire chiffrer l'information sensible IS_j par le module de sécurité au moyen d'une clé de protection temporaire de chiffrement CPI dans une version actuelle $CPI_{(ai+1)}$ fournie par le module de sécurité et d'un algorithme de chiffrement stocké, avec un algorithme de déchiffrement associé, dans lesdits moyens de

10 mémorisation ;

-faire stocker par le module de sécurité, dans une mémoire non volatile (10) de celui-ci, l'information sensible sous forme chiffrée $\overline{IS_j}_{(ai+1)}$ associée à des données d'identification définissant une clé de protection temporaire de déchiffrement $CPid$ dans une version actuelle $CPid_{(ai+1)}$ associée à ladite version

15 actuelle $CPI_{(ai+1)}$ de la clé de protection temporaire de chiffrement CPI , lesdites données d'identification comprenant une identité de clé $CPid$ et un indice de mise à jour $(ai+1)$ qui définit ladite version actuelle $CPid_{(ai+1)}$ de la clé de déchiffrement parmi plusieurs versions ; et

-dans le cas où la clé de protection temporaire de déchiffrement $CPid$ dans sa version actuelle $CPid_{(ai+1)}$ n'est pas déjà stockée dans ladite mémoire non volatile (10), faire stocker cette version par le module de sécurité.

20

2. Procédé de stockage selon la revendication 1, dans lequel le module de sécurité comprend des moyens de génération d'aléa fournissant des versions

25 successives différentes d'un aléa, chaque version de la clé de protection temporaire de chiffrement CPI fournie par le module de sécurité étant obtenue à partir d'une version différente dudit aléa.

3. Procédé d'exploitation d'une information sensible IS_j dans un module de sécurité (8) comprenant des moyens de traitement de l'information (9) et des

30 moyens de mémorisation de l'information (10,14), cette information sensible IS_j étant sous une forme chiffrée par le module de sécurité au moyen d'une clé de protection temporaire de chiffrement CPI dans une version actuelle $CPI_{(ai+1)}$ fournie par le module de sécurité et d'un algorithme de chiffrement stocké, avec un

algorithme de déchiffrement associé, dans lesdits moyens de mémorisation, l'information sensible sous forme chiffrée $\overline{ISj}_{(ai+1)}$ étant stockée dans une mémoire non volatile (10) du module de sécurité en association avec des données d'identification définissant une clé de protection temporaire de déchiffrement CPid dans une version actuelle CPid_(ai+1) associée à ladite version actuelle CPi_(ai+1) de la clé de protection temporaire de chiffrement CPi, lesdites données d'identification comprenant une identité de clé CPid et un indice de mise à jour (ai+1) qui définit ladite version actuelle CPid_(ai+1) de la clé de déchiffrement parmi plusieurs versions, caractérisé en ce qu'il comprend les étapes consistant à :

- 10 -faire sélectionner par le module de sécurité, lors d'une demande d'utilisation de l'information sensible ISj émanant de l'intérieur ou de l'extérieur de celui-ci, ladite version actuelle CPid_(ai+1) de la clé de protection temporaire de déchiffrement CPid associée à cette information sensible, au moyen desdites données d'identification ;
- 15 -faire déchiffrer par le module de sécurité l'information sensible chiffrée $\overline{ISj}_{(ai+1)}$, au moyen de la version actuelle CPid_(ai+1) de la clé de protection temporaire de déchiffrement CPid et de l'algorithme de déchiffrement, et stocker provisoirement l'information sensible ISj sous une forme déchiffrée ainsi obtenue de telle façon qu'elle disparaisse du module de sécurité après une utilisation de
- 20 cette information sensible ; et
- faire utiliser par le module de sécurité l'information sensible ISj sous sa forme déchiffrée.

4. Procédé d'exploitation selon la revendication 3, pour modifier périodiquement la forme chiffrée d'une information sensible, comprenant les étapes consistant à :

- faire déchiffrer par le module de sécurité l'information sensible stockée sous une forme chiffrée actuelle $\overline{ISj}_{(ai+1)}$, au moyen de la version actuelle CPid_(ai+1) de la clé de protection temporaire de déchiffrement CPid qui lui est associée et
- 30 dudit algorithme de déchiffrement ;
- faire sélectionner par le module de sécurité une nouvelle version CPi_(ai+2) de la clé de protection temporaire de chiffrement CPi ; puis

-faire rechiffrer par le module de sécurité l'information sensible déchiffrée IS_j au moyen de la nouvelle version $CPI_{(ai+2)}$ de la clé de protection temporaire de chiffrement et dudit algorithme de chiffrement pour produire une nouvelle forme chiffrée $\overline{IS_j}_{(ai+2)}$ de l'information sensible ; et

- 5 -stocker, dans le module de sécurité, l'information sensible sous sa nouvelle forme chiffrée $\overline{IS_j}_{(ai+2)}$ et une nouvelle version $CPid_{(ai+2)}$ de la clé de protection temporaire de déchiffrement $CPid$ associée à ladite nouvelle version $CPI_{(ai+2)}$ de la clé de protection temporaire de chiffrement.

- 10 5. Procédé d'exploitation selon la revendication 4, dans lequel le module de sécurité comprend des moyens de génération d'aléa fournissant des versions successives différentes d'un aléa, chaque version actuelle $CPI_{(ai+1)}$ et nouvelle version $CPid_{(ai+2)}$ de la clé de protection temporaire de chiffrement CPI fournie par le module de sécurité étant obtenue à partir d'une version différente dudit aléa.

- 15 6. Procédé d'exploitation selon la revendication 4, dans lequel on stocke dans la mémoire non volatile (10) du module de sécurité deux versions les plus récentes de chaque clé de protection temporaire de déchiffrement $CPid$, à savoir une avant-dernière version $CPid_{ai}$ et une dernière version $CPid_{(ai+1)}$ et, lorsqu'une
20 nouvelle version $CPI_{(ai+2)}$ d'une quelconque clé de protection temporaire de chiffrement est produite par le module de sécurité, on fait stocker par celui-ci dans la mémoire non volatile (10) une nouvelle version correspondante $CPid_{(ai+2)}$ de la clé de protection temporaire de déchiffrement $CPid$ associée, à la place de l'avant-dernière version $CPid_{ai}$.

- 25 7. Procédé d'exploitation selon la revendication 6, dans lequel on chiffre plusieurs informations sensibles $IS(j-1)$, IS_j respectivement avec une avant-dernière version CPI_{ai} et une dernière version $CPI_{(ai+1)}$ différentes d'une même clé de protection temporaire de chiffrement CPI pour donner des formes chiffrées
30 $\overline{IS(j-1)}_{ai}$ et $\overline{IS_j}_{(ai+1)}$ et, lorsqu'une nouvelle version de ces informations sensibles doit être produite par le module de sécurité, on exécute les étapes suivantes :

-faire déchiffrer par le module de sécurité les informations sensibles $\overline{IS(j-1)}_{ai}$ chiffrées avec l'avant-dernière version CPI_{ai} de la clé de protection

temporaire chiffrement CPI , au moyen de l'avant-dernière version $CPid_{ai}$ de la clé de protection temporaire de déchiffrement $CPid$ qui lui est associée ;

- faire rechiffrer par le module de sécurité les informations sensibles déchiffrées $IS(j-1)$ au moyen de ladite dernière version $CPI_{(ai+1)}$ de la clé de protection temporaire de chiffrement pour produire une nouvelle forme chiffrée $\overline{IS(j-1)}_{(ai+1)}$ de l'information sensible ; et

-stocker, dans le module de sécurité, ces informations sensibles sous leur nouvelle forme chiffrée $\overline{IS(j-1)}_{(ai+1)}$; et, pour produire ladite nouvelle version des informations sensibles $IS(j-1)$, ISj , on exécute les étapes suivantes :

- faire déchiffrer par le module de sécurité toutes les informations sensibles $\overline{IS(j-1)}_{(ai+1)}$ et $\overline{ISj}_{(ai+1)}$ relatives à ladite clé de protection temporaire de chiffrement CPI au moyen d'une dernière version $CPid_{(ai+1)}$ de la clé de protection temporaire de déchiffrement $CPid$ associée à ladite dernière version $CPI_{(ai+1)}$ de la clé de protection temporaire de chiffrement CPI

- faire rechiffrer par le module de sécurité les informations sensibles déchiffrées $IS(j-1)$, ISj , au moyen d'une nouvelle version $CPI_{(ai+2)}$ de la clé de protection temporaire de chiffrement et dudit algorithme de chiffrement pour produire une nouvelle forme chiffrée $\overline{IS(j-1)}_{(ai+2)}$ et $\overline{ISj}_{(ai+2)}$ de ces informations sensibles ; et

- stocker, dans le module de sécurité, ces informations sensibles sous leur nouvelle forme chiffrée $\overline{IS(j-1)}_{(ai+2)}$ et $\overline{ISj}_{(ai+2)}$ et une nouvelle version $CPid_{(ai+2)}$ de la clé de protection temporaire de déchiffrement $CPid$ associée à ladite nouvelle version $CPI_{(ai+2)}$ de la clé de protection temporaire de chiffrement.

8. Module de sécurité (8) comprenant des moyens de traitement de l'information (9) et des moyens de mémorisation de l'information (10,14), caractérisé en ce qu'il comprend :

- des moyens de production de clés agencés pour produire une ou plusieurs clés de protection temporaires de chiffrement $CP1, \dots, CPI, \dots, CPn$ et autant de clés de protection temporaires de déchiffrement associées $CP1d, \dots, CPid, \dots, CPnd$ et, pour chaque clé de protection temporaire de chiffrement CPI et de déchiffrement $CPid$, plusieurs versions successives CPI_{ai} , $CPI_{(ai+1)}$, $CPI_{(ai+2)}$ et $CPid_{ai}$, $CPid_{(ai+1)}$, $CPid_{(ai+2)}$;

-des moyens agencés pour associer à une information sensible déterminée IS_j une clé de protection temporaire de chiffrement CP_i déterminée et une clé de protection temporaire de déchiffrement CP_{id} associée à la clé de protection temporaire de chiffrement CP_i ;

- 5 -des moyens de chiffrement agencés pour effectuer des chiffrements successifs de l'information sensible IS_j en utilisant l'une ou l'autre desdites versions successives CP_{i_{ai}} , CP_{i_(ai+1)} , CP_{i_(ai+2)} de la clé de protection temporaire de chiffrement associée à cette information sensible et un algorithme de chiffrement stocké dans les moyens de mémorisation (10,14) ; et
- 10 -des moyens de déchiffrement agencés pour effectuer des déchiffrements successifs de l'information sensible IS_j en utilisant à chaque déchiffrement, parmi lesdites versions successives CP_{id_{ai}} , CP_{id_(ai+1)} , CP_{id_(ai+2)} de la clé de protection temporaire de déchiffrement, celle qui est associée à la version de la clé de protection temporaire de chiffrement utilisée pour le chiffrement correspondant, et
- 15 un algorithme de déchiffrement stocké dans les moyens de mémorisation (10,14).

9. Module de sécurité selon la revendication 8, qui comprend des moyens de génération d'aléa fournissant des versions successives différentes d'un aléa, chacune desdites versions successives CP_{i_{ai}} , CP_{i_(ai+1)} , CP_{i_(ai+2)} de chaque clé de protection temporaire de chiffrement CP_i fournie par le module de sécurité étant
- 20 obtenue à partir d'une version différente dudit aléa.

1/5

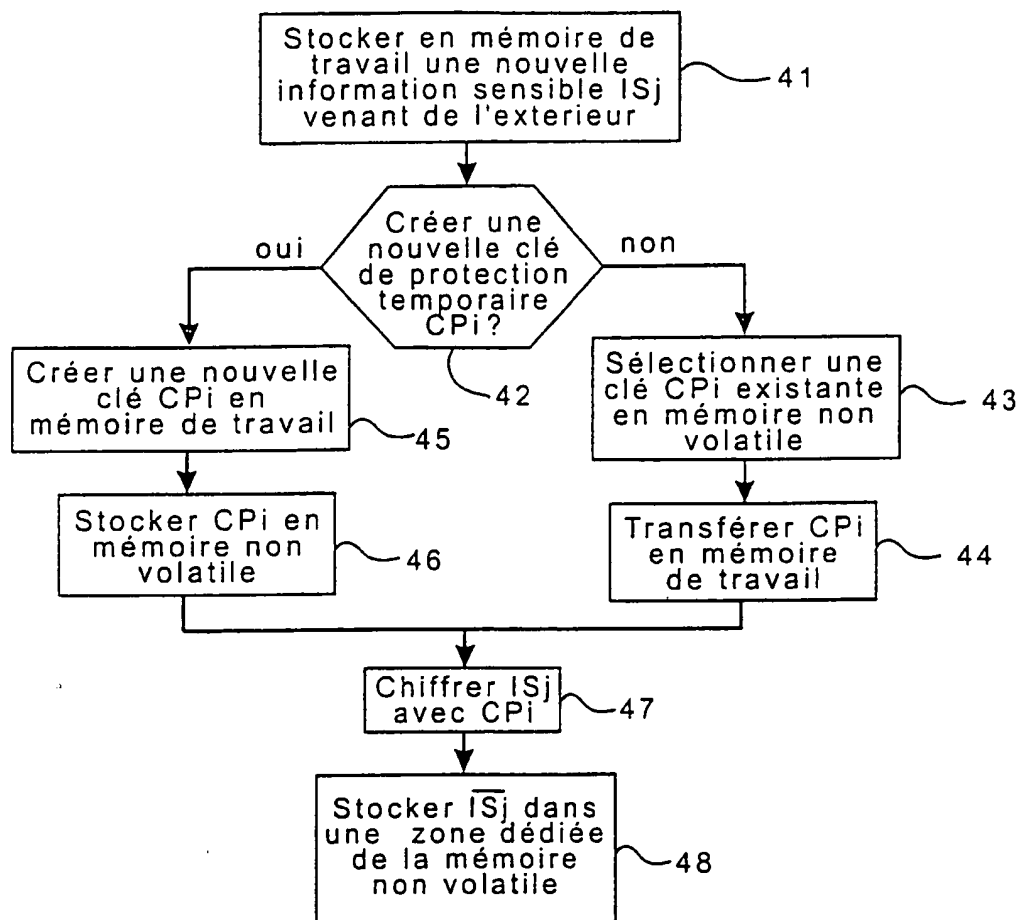


Fig.4

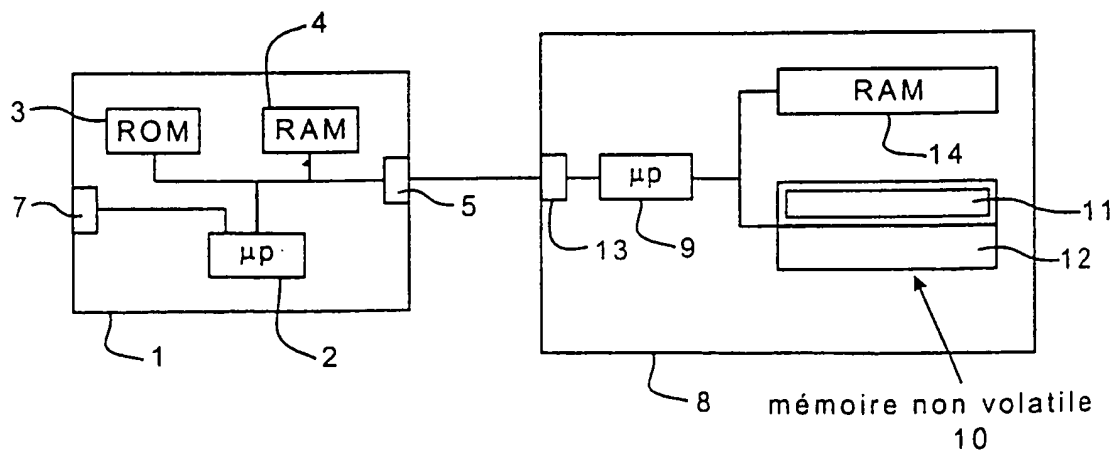


Fig.1

2 / 5

clés de protection temporaires	numéro de clé	indice de mise à jour	valeur stockée de la clé
CP1	N1	a1	CP1 _{a1}
		a1+1	CP1 _(a1+1)
.	.	.	.
.	.	.	.
.	.	.	.
CPi	Ni	ai	CPi _{ai}
		ai+1	CPi _(ai+1)
.	.	.	.
.	.	.	.
.	.	.	.
CPn	Nn	an	CPn _{an}
		an+1	CPn _(an+1)

Fig. 2

Référence des informations sensibles	Numéro de la clé associée	Indice actuel de la clé	version stockée de l'information sensible
IS1	N1	a1+1	$\overline{IS1}_{(a1+1)}$
IS2	N1	a1+1	$\overline{IS1}_{(a1+1)}$
.	.	.	.
.	.	.	.
.	.	.	.
IS(j-1)	Ni	ai	$\overline{IS(j-1)}_{ai}$
ISj	Ni	ai+1	$\overline{ISj}_{(ai+1)}$
.	.	.	.
.	.	.	.
.	.	.	.
ISm	Nn	an+1	$\overline{ISm}_{(an+1)}$

Fig. 3

3/5

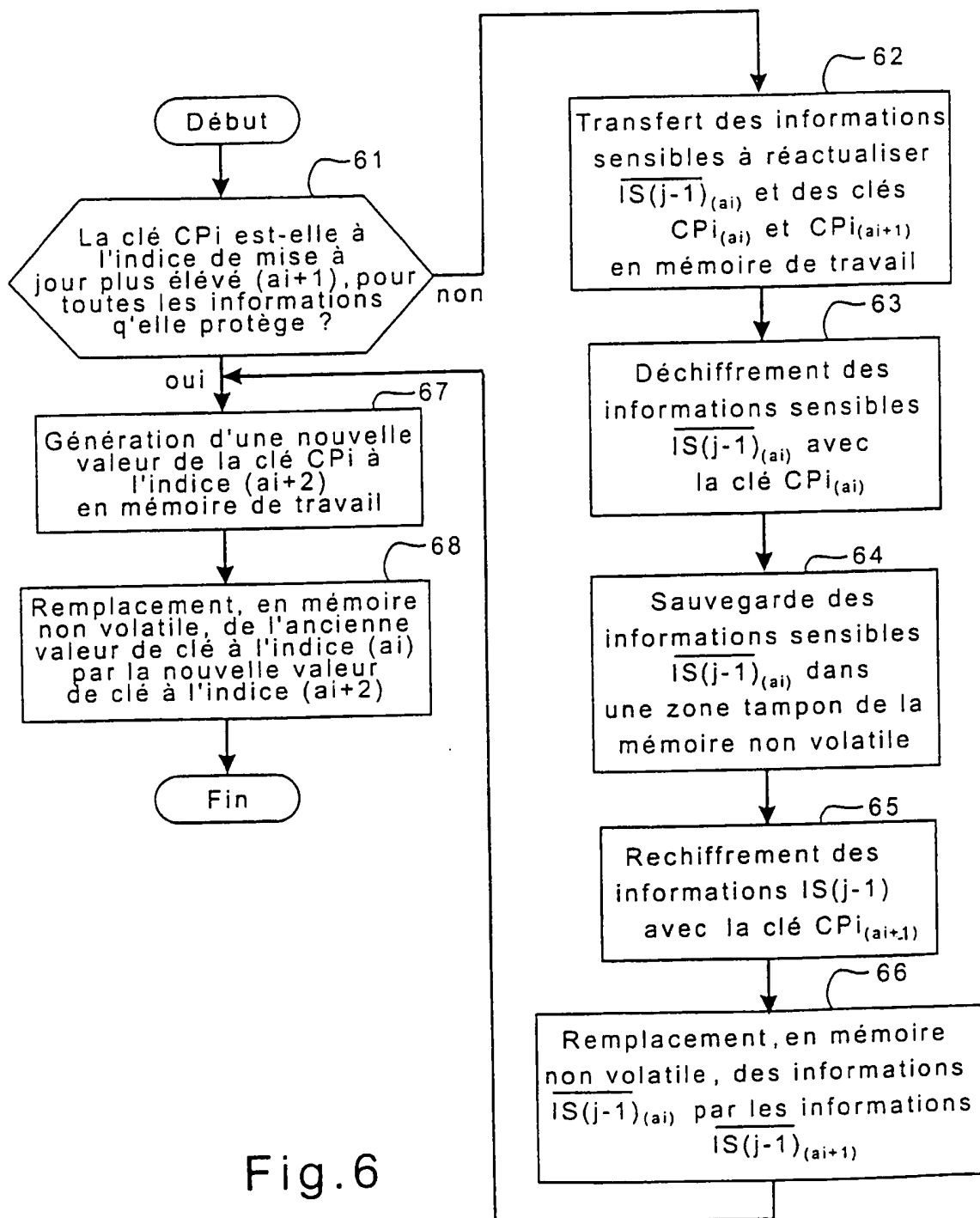


Fig.6

4/5

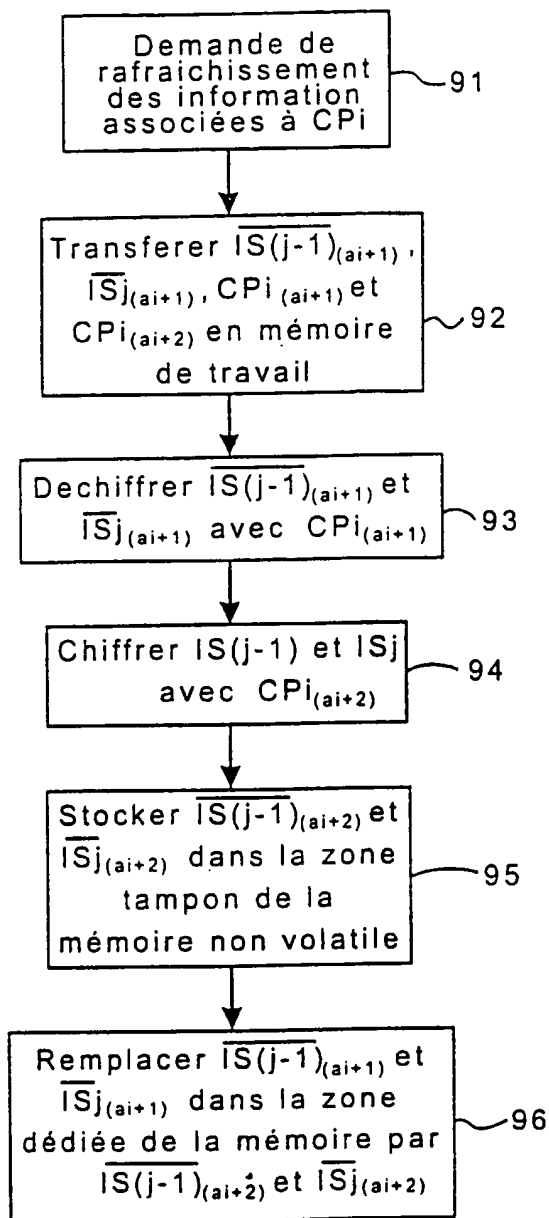


Fig.9

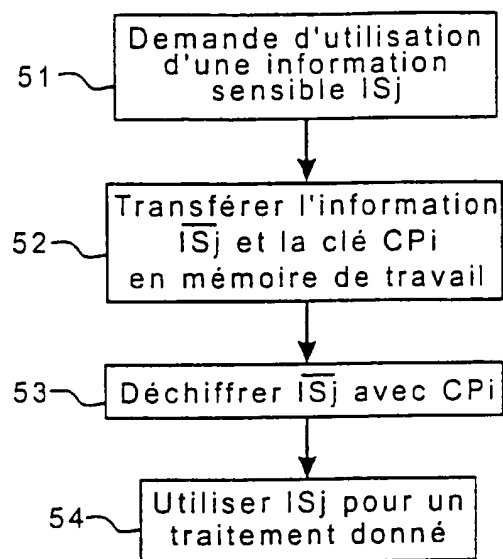


Fig.5

5 / 5

clés de protection temporaires	numéro de clé	indice de mise à jour	valeur stockée de la clé
CP1	N1	a1	CP1 _{a1}
		a1+1	CP1 _(a1+1)
.	.	.	.
.	.	.	.
.	.	.	.
CPi	Ni	ai+2	CPi _(ai+2)
		ai+1	CPi _(ai+1)
.	.	.	.
.	.	.	.
.	.	.	.
CPn	Nn	an	CPn _{an}
		an+1	CPn _(an+1)

Fig. 7

Référence des informations sensibles	Numéro de la clé associée	Indice actuel de la clé	version stockée de l'information sensible	Nouvel Indice de la clé	nouvelle version stockée de l'information sensible
IS1	N1	a1+1	$\overline{IS1}_{(a1+1)}$		
IS2	N1	a1+1	$\overline{IS1}_{(a1+1)}$		
.
.
.
IS(j-1)	Ni	ai+1	$\overline{IS(j-1)}_{(ai+1)}$	ai+2	$\overline{IS(j-1)}_{(ai+2)}$
ISj	Ni	ai+1	$\overline{ISj}_{(ai+1)}$	ai+2	$\overline{ISj}_{(ai+2)}$
.
.
.
ISm	Nn	an+1	$\overline{ISm}_{(an+1)}$		

Fig. 8

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 98/00503

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 621 569 A (BULL CP8) 26 October 1994 see abstract; claims; figures ---	1,3,8
A	EP 0 002 390 A (IBM) 13 June 1979 see abstract; claims; figure 1 ---	1,3,8
A	EP 0 186 981 A (IBM) 9 July 1986 see abstract; claims; figures see column 7, line 20 - column 8, line 61 ---	1-5,8
A	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) 12 March 1993 see abstract; claims; figures ---	1-5,8
A	EP 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS) 14 August 1991 ---	
A	WO 96 07994 A (BANKSYS) 14 March 1996 -----	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

9 July 1998

Date of mailing of the international search report

17/07/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

David, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/00503

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0621569 A	26-10-1994	FR 2704341 A	28-10-1994
		AU 673900 B	28-11-1996
		AU 6057994 A	03-11-1994
		CA 2121410 A	23-10-1994
		CN 1100219 A,B	15-03-1995
		JP 2710754 B	10-02-1998
		JP 7013873 A	17-01-1995
		KR 9700845 B	20-01-1997
		NO 941460 A	24-10-1994
		US 5533126 A	02-07-1996
EP 0002390 A	13-06-1979	US 4203166 A	13-05-1980
		CA 1121013 A	30-03-1982
		JP 1281000 C	13-09-1985
		JP 54087032 A	11-07-1979
		JP 60003655 B	30-01-1985
EP 0186981 A	09-07-1986	GB 2168514 A	18-06-1986
		DE 3585439 A	02-04-1992
		JP 61139878 A	27-06-1986
		US 4731842 A	15-03-1988
FR 2681165 A	12-03-1993	NONE	
EP 0440800 A	14-08-1991	JP 2731945 B	25-03-1998
		JP 3007399 A	14-01-1991
		WO 9014962 A	13-12-1990
WO 9607994 A	14-03-1996	BE 1008699 A	02-07-1996
		AU 687622 B	26-02-1998
		AU 3377895 A	27-03-1996
		CA 2199504 A	14-03-1996
		EP 0780012 A	25-06-1997
		NO 971066 A	09-05-1997

RAPPORT DE RECHERCHE INTERNATIONALE

De l' le Internationale No

PCT/FR 98/00503

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 621 569 A (BULL CP8) 26 octobre 1994 voir abrégé; revendications; figures ---	1,3,8
A	EP 0 002 390 A (IBM) 13 juin 1979 voir abrégé; revendications; figure 1 ---	1,3,8
A	EP 0 186 981 A (IBM) 9 juillet 1986 voir abrégé; revendications; figures voir colonne 7, ligne 20 - colonne 8, ligne 61 ---	1-5,8
A	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) 12 mars 1993 voir abrégé; revendications; figures ---	1-5,8
A	EP 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS) 14 août 1991 ---	
	-/--	

☒ Voir la suite du cadre C pour la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

9 juillet 1998

Date d'expédition du présent rapport de recherche internationale

17/07/1998

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

David, J

RAPPORT DE RECHERCHE INTERNATIONALE

Der. le Internationale No
PCT/FR 98/00503

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 07994 A (BANKSYS) 14 mars 1996 -----	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Der le Internationale No

PCT/FR 98/00503

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0621569 A	26-10-1994	FR 2704341 A	28-10-1994
		AU 673900 B	28-11-1996
		AU 6057994 A	03-11-1994
		CA 2121410 A	23-10-1994
		CN 1100219 A,B	15-03-1995
		JP 2710754 B	10-02-1998
		JP 7013873 A	17-01-1995
		KR 9700845 B	20-01-1997
		NO 941460 A	24-10-1994
		US 5533126 A	02-07-1996
EP 0002390 A	13-06-1979	US 4203166 A	13-05-1980
		CA 1121013 A	30-03-1982
		JP 1281000 C	13-09-1985
		JP 54087032 A	11-07-1979
		JP 60003655 B	30-01-1985
EP 0186981 A	09-07-1986	GB 2168514 A	18-06-1986
		DE 3585439 A	02-04-1992
		JP 61139878 A	27-06-1986
		US 4731842 A	15-03-1988
FR 2681165 A	12-03-1993	AUCUN	
EP 0440800 A	14-08-1991	JP 2731945 B	25-03-1998
		JP 3007399 A	14-01-1991
		WO 9014962 A	13-12-1990
WO 9607994 A	14-03-1996	BE 1008699 A	02-07-1996
		AU 687622 B	26-02-1998
		AU 3377895 A	27-03-1996
		CA 2199504 A	14-03-1996
		EP 0780012 A	25-06-1997
		NO 971066 A	09-05-1997